Cyberattacks on hospitals are likely to increase, putting lives at risk, experts warn

February 14 2024, by Amanda Seitz

Lurie Children's Hospital sign is seen at the hospital as patients walk in, Feb. 5, 2024, in Skokie, Ill. A cyberattack on a renowned children's hospital in Chicago has left some parents scrambling. They've had to reschedule surgeries on babies or scramble to get prescriptions filled for their sick kids. Experts warn this is just the start of a growing trend of foreign criminals attacking U.S. hospitals for hefty ransoms. Credit: AP Photo/Nam Y. Huh, File

Cybersecurity experts are warning that hospitals around the country are at risk for attacks like the one that is crippling operations at a premier Midwestern children's hospital, and that the U.S. government is doing too little prevent such breaches.

Hospitals in recent years have shifted their use of online technology to support everything from telehealth to medical devices to patient records. Today, they are a favorite target for internet thieves who hold systems' data and networks hostage for hefty ransoms, said John Riggi, the American Hospital Association's cybersecurity adviser.

"Unfortunately, the unintended consequence of the use of all this network and internet connected technology is it expanded our digital attack surface," Riggi said. "So, many more opportunities for bad guys to penetrate our networks."

The assailants often operate from American adversaries such as Russia, North Korea and Iran, where they enjoy big payouts from their victims and face little prospect of ever being punished.

In November, a ransomware attack on a health care chain that operates 30 hospitals and 200 health facilities in the United States forced doctors to divert patients from emergency rooms and postpone elective surgeries. Meanwhile, a rural Illinois hospital announced it was permanently closing last year because it couldn't recover financially from a cyberattack. And hackers went as far as posting photos and patient information of breast cancer patients who were receiving treatment at a Pennsylvania health network after the system was hacked last year.

Now, one of the top children's hospitals in the country, the Ann & Robert H. Lurie Children's Hospital of Chicago, has been forced to put its phone, email and medical record systems offline as it battles a cyberattack. The FBI has said it is investigating.

Brett Callow, an analyst for the cybersecurity firm Emsisoft, counted 46 cyberattacks on hospitals last year, compared with 25 in 2022. The paydays for criminals have gotten bigger too, with the average payout jumping from $5,000 in 2018 to $1.5 million last year.

The Lurie Children's Hospital sign is displayed at the hospital, Feb. 5, 2024, in Skokie, Ill. A cyberattack on a renowned children's hospital in Chicago has left some parents scrambling. They've had to reschedule surgeries on babies or scramble to get prescriptions filled for their sick kids. Experts warn this is just the start of a growing trend of foreign criminals attacking U.S. hospitals for hefty ransoms. Credit: AP Photo/Nam Y. Huh, File

"Unless governments do something more meaningful, more significant

than they have done to date, it's inevitable that it'll get worse," Callow said.

Callow believes the government should ban cyberattack victims such as hospitals, local governments and schools from paying ransoms. "There's so much money being paid into the ransomware system now there's no way the problem is going to simply go away on itself," he said.

The dramatic increase in these online raids has prompted the nation's top health agency to develop new rules for hospitals to protect themselves from cyber threats.

The Department of Health and Human Services said it will rewrite the rules for the Health Insurance Portability and Accountability Act -– the federal law commonly called HIPPA that requires insurers and health systems to protect patient information—to include new provisions that address cybersecurity later this year.

The department is also considering new cybersecurity requirements attached to hospitals' Medicaid and Medicare funding.

"The more prepared we are the better," said Deputy Secretary Andrea Palm.

But, she added, some hospitals will struggle to protect themselves. She is worried about rural hospitals, for example, that may have difficulty cobbling together money to properly update their cybersecurity. HHS wants more money from Congress to tackle the issue, but Palm said the agency doesn't have a precise dollar amount its seeking.

Lurie Children's Hospital logo is seen at the hospital, Feb. 5, 2024, in Skokie, Ill. A cyberattack on a renowned children's hospital in Chicago has left some parents scrambling. They've had to reschedule surgeries on babies or scramble to get prescriptions filled for their sick kids. Experts warn this is just the start of a growing trend of foreign criminals attacking U.S. hospitals for hefty ransoms. Credit: AP Photo/Nam Y. Huh, File

"It's important to note that this has to come with resources," Palm said. "We can't set the industry up not to be able to meet requirements."

Becoming the victim of a cyberattack is costly, too. The attacks can put hospitals' networks offline for weeks or months, forcing hospitals to turn away patients.

In Chicago, Lurie hospital's network has been offline for two weeks. The hospital, which served more than 260,000 patients last year, has established a separate call center for patients' needs and resumed some care.

On Thursday, Lurie's surgeons operated on Jason Castillo's 7-month-old daughter mostly by hand, without some of the high-tech devices usually used.

His daughter's planned heart surgery was postponed on Jan. 31, when the hospital found itself under cyber siege. The surgeon talked to Castillo before his daughter was wheeled in for a six-hour surgery, promising that he felt confident he could do the procedure despite the ongoing cyberattack.

"She's doing fantastic," Castillo said of his daughter, who is now recovering at home. "It feels like a huge cloud has been lifted from our household."

Even once Lurie has restored their network, it'll likely take months of behind-the-scenes work for the hospital to fully rebound, Callow said.

"These incidents can affect everything from patient care to payroll," Callow said. "Fully recovering can take months, it's not simply a matter of flicking a switch and everything comes back on."

Citation: Cyberattacks on hospitals are likely to increase, putting lives at risk, experts warn (2024, February 14) retrieved 6 May 2024 from https://techxplore.com/news/2024-02-cyberattacks-hospitals-experts.html